AMENDMENTS TO THE DRAWINGS

The Examiner has objected to the drawings. Such objection is deemed avoided by virtue of the replacement sheets submitted herewith.

REMARKS

The Examiner has rejected Claims 1-17 under 35 U.S.C. 101 as being directed toward non-statutory subject matter. Applicant has clarified Claim 1 to include a computer program product "embodied on a tangible computer readable medium" in order to avoid such rejection.

The Examiner has rejected Claims 1-51 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The Examiner begins by taking issue with the following language from Claims 1, 7, 18, 24, 35 and 41 as being indefinite: "more strongly." Applicant respectfully asserts that such claim language is to be read according to the plain and ordinary meaning thereof, in view of dictionary definitions, etc. The Examiner argues that "it is uncertain what the association is stronger than." In response, applicant respectfully asserts that the association is stronger than it would be without the modification of the set of rules.

The Examiner continues by arguing that there is insufficient antecedent basis for the following limitation: "score values within said set of rules associated with said secondary set of one or more external program calls." In response, applicant has clarified Claims 7, 24 and 41 in order to avoid such rejection.

The Examiner has rejected Claims 1, 2, 8-10, 13, 14, 17, 18, 19, 25-27, 30, 34, 35, 36, 42-44, 47, 48 and 51 under 35 U.S.C. 102(e) as being anticipated by van der Made (U.S. Patent No. 7,093,239). Applicant respectfully disagrees with such rejection.

With respect to independent claims 1, 18 and 35, the Examiner has relied on Col. 6, lines 12-24; and Col. 11, lines 46-60 from the Made reference to make a prior art showing of applicant's claimed "secondary set identifying code operable to identify, within said stream, at least one secondary set of one or more external program calls

associated with said primary set of one or more external program calls" (see this or similar, but not necessarily identical language in the independent claims).

Applicant respectfully points out that the Made reference excerpts relied upon by the Examiner merely teach "extracting a behavior pattern and sequence from a modified, new, unknown or suspect program," and that "[t]he behavior pattern is preferably used to analyze the behavior of the unknown program to determine if the behavior of the unknown program is malicious" (Col. 6, lines 13-17 – emphasis added). The excerpts from Made also teach that the "ABM engine then analyzes the first executable program and finds that its behavior pattern is altered in a manner indicating that a virus is active" (Col. 11, lines 57-59 – emphasis added).

However, applicant respectfully asserts that only generally disclosing that "[t]he behavior pattern is preferably used to analyze the behavior of the unknown program," as in Made, does not specifically meet a "secondary set of identifying code operable to identify, within said stream, at least one secondary set of one or more external program calls associated with said primary set of one or more external program calls" (emphasis added), particularly where the "primary set of one or more external program calls match[es] one or more rules indicative of malicious computer program activity from among a set of rules" (emphasis added), in the context claimed by applicant.

Furthermore, applicant respectfully points out that detecting active viruses based on whether an executable program's behavior pattern is altered, as in Made, clearly fails to teach the use of a "secondary set of identifying code operable to identify, within said stream, at least one secondary set of one or more external program calls associated with said primary set of one or more external program calls" (emphasis added), where the "primary set of one or more external program calls match[es] one or more rules indicative of malicious computer program activity from among a set of rules" (emphasis added), in the context claimed by applicant. Simply nowhere in the excerpts relied on by the Examiner is there any teaching or suggestion of a "secondary set of one or more external

program calls associated with said primary set of one or more external program calls," as claimed.

Still with respect to independent claims 1, 18 and 35, the Examiner has again relied on Col. 6, lines 12-24; and Col. 11, lines 46-60 from the Made reference to make a prior art showing of applicant's claimed "modifying code operable to modify said set of rules such that said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity" (see this or similar, but not necessarily identical language in the independent claims).

Applicant respectfully points out that the Made reference excerpts relied upon by the Examiner merely teach "extracting a behavior pattern and sequence from a modified, new, unknown or suspect program," and that "[t]he behavior pattern is preferably used to analyze the behavior of the unknown program to determine if the behavior of the unknown program is malicious" (Col. 6, lines 13-17 – emphasis added). Such excerpts from Made also teach that the "ABM engine then analyzes the first executable program and finds that its behavior pattern is altered in a manner indicating that a virus is active" (Col. 11, lines 57-59 – emphasis added).

However, applicant respectfully asserts that analyzing "the behavior pattern of the unknown program," and detecting active viruses based on whether an executable program's behavior pattern is altered, as in Made, clearly fail to teach "modifying code operable to modify said set of rules such that said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity," (emphasis added), as claimed by applicant, particularly where the "rules [are] indicative of malicious computer program activity," in the context claimed. Simply nowhere in the Made excerpts relied on by the Examiner is there any teaching or suggestion to "modify said set of rules," as claimed by applicant.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a

single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Made reference, as noted above. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claims 2 et al., the Examiner has relied on Col. 6, lines 12-24 (excerpted below) from the Made reference to make a prior art showing of applicant's claimed technique "wherein one of said at least one secondary set of one or more external program calls precedes said primary set of one or more external program calls within said stream of external program calls."

> "Preferred implementations of the analytical behavior method (ABM) proceed by extracting a behavior pattern and sequence from a modified, new, unknown or suspect program. The behavior pattern is preferably used to analyze the behavior of the unknown program to determine if the behavior of the unknown program is malicious. Identification of malicious behavior in this manner allows identification of virus carrying files prior to infection of the host computer system. The behavior pattern can also be stored in a database and the virtual machine can subsequently analyze the behavior of the program following modification to determine if its functionality has been modified in a suspect (malicious) manner. This provides post-infection analysis." (Col. 6, lines 12-24 - emphasis added)

Applicant respectfully points out that the Made reference excerpt relied upon by the Examiner merely teaches "extracting a behavior pattern and sequence from a modified, new, unknown or suspect program," and that "[t]he behavior pattern is preferably used to analyze the behavior of the unknown program to determine if the behavior of the unknown program is malicious" (Col. 6, lines 13-17 – emphasis added).

However, applicant respectfully asserts that only generally disclosing that "[t]he behavior pattern is preferably used to analyze the behavior of the unknown program," as in Made, fails to specifically disclose a technique "wherein one of said at least one secondary set of one or more external program calls precedes said primary set of one or more external program calls within said stream of external program calls," as claimed by applicant.

In addition, with respect to Claims 14 et al., the Examiner has relied on Col. 11, lines 46-59 (excerpted below) from the Made reference to make a prior art showing of applicant's claimed technique "wherein said set of rules is modified to include a new rule corresponding to said secondary set of one or more external program calls, said new rule thereafter being used in addition to other rules within said set of rules."

> "Post-infection detection
>
> Post-infection detection takes place in cases when initial infection is missed by pre-infection detection. A virus could be missed by pre-infection detection when it does not perform any viral function on first execution and does not modify interrupt vectors that point to an infection routine. This is the case with so-called slow infectors and similarly behaving malignant code. In post-infection detection the virus is caught the moment it attempts to infect the first executable on the PC. The file hook mechanism detects this attempted change to an executable (including documents). The ABM engine then analyzes the first executable program and finds that its behavior pattern is altered in a manner indicating that a virus is active." (Col. 11, lines 46-59 - emphasis added)

Applicant respectfully points out that the Made reference excerpt relied upon by the Examiner merely teaches detecting a virus in an executable program if the program's "behavior pattern is altered in a manner indicating that a virus is active" (Col. 11, lines 58-59 – emphasis added).

However, applicant respectfully asserts that detecting an active virus in a program because the program's behavior pattern is altered, as in Made, clearly does not teach that a "set of rules is modified to include a new rule corresponding to said secondary set of one or more external program calls," especially where "said new rule thereafter [is] used

in addition to other rules within said set of rules" (emphasis added), as claimed by applicant.

In addition, with respect to Claims 17 et al., the Examiner has relied on Col. 12, lines 26-41 (excerpted below) from the Made reference to make a prior art showing of applicant's claimed technique "wherein said set of rules is subject to a validity check after modification to determine if said set of rules is more effectively detecting malicious computer program activity."

> "In tests of a prototype implementation ABM system, the combination of pre-infection (96%) and post-infection detection (4%) resulted in 100% detection of all known viral techniques, using a combination of new, modified and well-known viruses. Other methods detected only 100% of known viruses and scored as low as 0% for the detection of new, modified and unknown viruses. No exact figure can be quoted for tests involving signature scanner based products. The results for such products are a direct representation of the mix of known, modified and new, unknown viruses; e.g. if 30% of the virus test set is new, modified or unknown then the final score reflected close to 30% missed viruses. No such relationship exists for the implementations of preferred aspects of the present system, where the detection efficiency does not appreciably vary for alterations of the presented virus mix." (Col. 12, lines 26-41 - emphasis added)

Applicant respectfully points out that the Made reference excerpt relied upon by the Examiner merely discloses "tests of a prototype implementation ABM system, the combination of pre-infection (96%) and post-infection detection (4%) resulted in 100% detection of all known viral techniques, using a combination of new, modified and well-known viruses" (Col. 12, lines 26-41 – emphasis added).

However, applicant respectfully asserts that "tests of a prototype implementation ABM system," as in Made, clearly do not teach that a "set of rules is subject to a validity check after modification to determine if said set of rules is more effectively detecting malicious computer activity" (emphasis added), as claimed by applicant. Simply nowhere in the Made excerpt relied on by the Examiner is there any teaching or

suggestion of a "validity check after modification [of said set of rules]," as claimed by applicant.

Again, since the anticipation criterion has simply not been met by the Made reference, as noted above, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 52-53 below, which are added for full consideration:

> "applying high level rules to the modified set of rules, and promoting said modified set of rules from a temporary set to a permanent set based on the application of the high level rules to the modified set of rules" (see Claim 52); and
>
> "determining whether said modified set of rules decrease malicious network traffic, and promoting said modified set of rules from a temporary set to a permanent set if it is determined that said modified set of rules decrease said malicious network traffic" (see Claim 53).

Again, a notice of allowance or a proper prior art showing of <u>all</u> of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The

Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P489).

Respectfully submitted,
Zilka-Kotab, PC

/KEVINZILKA/

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100